Hazeldown Primary School
Maudlin Drive,Teignmouth TQ14 8SE
Tel 01626 772901
admin@hazeldown.devon.sch.uk
www.hazeldown.co.uk

GDPR Breach and Escalation Procedure

This policy was adopted by the School Governing Body on

12th February 2020

Review Date: February2021

Stephens Scown LLP, Curzon House, Southernhay West, Exeter EX1 1RS
T: 01392 210700 **F:** 01392 274010 **DX:** 8305 Exeter **W:** Stephens-scown.co.uk

Ref: ***TCM/BP/EXET-85-1***

CONTENTS

1. **DEFINITIONS**

The following definitions apply in this policy:

DPO	Data Protection Officer
ICO	Information Commissioners Office
GDPR	General Data Protection Regulation
School	Hazeldown School
Employee	All employees, officers, consultants, contractors, volunteers, interns, casual workers, and agency workers of the School.

2. **POLICY BACKGROUND AND PURPOSE**

2.1 This policy covers all employees, officers, consultants, contractors, volunteers, interns, casual workers, and agency workers. The term “employees” is used to refer to all such people listed in this clause.

2.2 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2.3 Data breach is one of the biggest fears that businesses face today. The School is committed to securing all data that it is responsible for and that all staff share this responsibility. It is important that any breach is dealt with immediately and effectively.

2.4 This policy sets out how the School complies with the data protection legislation (including, but not limited to, the GDPR), confidentiality issues and information security requirements in the event of a loss of personal data.

3. **APPLICATION AND RESPONSIBILITY**

3.1 All employees must familiarise themselves and comply with this Policy and related procedures. Failure to comply with this Policy and the related procedures will result in disciplinary action. The serious nature of data breaches, the significant risks of fines, enforcement action, reputational damage and disciplinary action, means that everyone in the organisation must play a part in compliance.

3.2 All employees are responsible for ensuring that all types of data are properly protected and kept secure.

4. **DATA PROTECTION AND GDPR**

4.1 Both data controllers and data processors must take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Failure to do so can result in individuals loosing control of their personal information. The GDPR also allows for the ICO to issue fines of up to €20m or 4% of annual turnover, whichever is greater. In addition, there would also be a detrimental affect to the School’s reputation from any negative press and increased operating costs after the fine. Failure to report a breach is a fineable offence.

5. DATA SECURITY BREACH OR POTENTIAL LOSS OF PERSONAL DATA

5.1 If an employee become aware of any:

- loss or potential loss of personal data;
- breach or potential breach of confidentiality;
- loss of laptop, tablet or other device, e.g. smartphone or mobile phone (whether it belongs to the School or to an employee personally), which may result in a loss of data or breach of confidentiality;
- breach of information security, whether physical or electronic;

the employee must immediately inform the Privacy Officer (PO) so that appropriate action can be taken and serious breaches reported.

5.2 To enable the PO to determine whether the breach is serious, the employee must provide all relevant information as requested by PO.

5.3 On receipt of the report, the PO, will respond to the incident and manage all communication. Under no circumstances should an employee engage in communication with another employee or any third party in relation to the breach. Specifically, employees must not report a breach to the ICO unless they have been directed to do so in writing by the PO.

6. ESCALATION PROCEDURE

Containment and Recovery

6.1 The PO will:

6.1.1 Investigate the breach in conjunction, with assistance as necessary, and ensure they have appropriate resources to properly investigate the breach;

6.1.2 Establish who needs to be made aware of the breach and inform them of what they must do to assist in any containment action required;

6.1.3 Establish whether anything can be done to recover any lost data and for to limit the damage caused by the breach;

6.1.4 Identify any third party involved in the breach and liaise with them, as appropriate;

6.1.5 Where appropriate, inform the police and the ICO.

Assessing the Risks

6.2 The PO will assess the risks which may be associated with the breach before taking any steps after the immediate containment, as follows:

6.2.1 What type of data is involved?

6.2.2 How sensitive is the data?

6.2.3 If the data has been lost or stolen, is there any protection, e.g. encryption?

6.2.4 What has happened to the data?

6.2.5 How could the data be misused?

6.2.6 How many individuals are affected?

6.2.7 Who are the individuals affected?

6.2.8 What harm can come to those individuals as a result of the loss / breach?

6.2.9 How serious / substantial is the harm?

6.2.10 How likely is it that any harm will happen?

6.2.11 Are there wider consequences to consider?

6.2.12 If an individual's bank details have been lost, what steps can be taken to prevent fraud?

6.3 Depending on the conclusion the PO will decide who needs to be notified.

Notification of Breaches

6.4 The PO will consider the following in determining whether (and whom) to notify:

6.4.1 legal / contractual requirements.

6.4.2 Will notification help to meet the obligation to report in relation to the GDPR?

6.4.3 Can notification help the individual?

6.4.4 Once we have established the severity of the resulting risk to people's rights and freedoms, the ICO can be informed.

6.4.5 How notification can be made appropriate for particular groups of individuals, e.g. vulnerable adults.

6.4.6 The dangers of over-notifying.

6.5 The PO will consider the following before deciding who to notify, what information to provide and how the information is to be communicated.

6.6 Any decision to report to the insurers (and what information to provide) will be taken by the PO.

Evaluation and Response Phase

6.7 The PO will evaluate the effectiveness of the School's response to the breach by considering the following:

6.7.1 What was the cause of the breach / reason for the loss?

6.7.2 What steps can be taken to prevent a recurrence?

6.7.3 Was the response hampered by inadequate policies or a lack of a clear allocation of responsibility?

6.7.4 Could existing procedures lead to another breach?

6.7.5 Where can improvements be made to the systems and controls?

6.8 The PO should ensure that they:

6.8.1 Know what personal data is held, where and how it is stored;

6.8.2 Establish where the major risks are and why, how much sensitive personal data is held, is data stored across the business or concentrated in one location;

6.8.3 Consider the risks involved in sharing data with or disclosing data to others; whether the method of transmission is secure; whether the minimum amount of data being shared / disclosed which data controllers / data processors / third parties the School shares with and whether the contracts need to be amended / improved;

6.8.4 Identify weak points in the existing security measures such as the use of portable storage devices;

6.8.5 Monitor employees' awareness of security issues and address any gaps through training or tailored advice;

6.8.6 Consider whether to establish a working group of employees to discuss "what if" scenarios to highlight risks and weaknesses and provide an opportunity for employees to suggest solutions;

6.8.7 Implement and test a Business Continuity Plan for data security breaches;

6.8.8 Identify a group of people responsible for reacting to reports of breaches of security or significant data loss.